North Staffordshire Combined Healthcare NHS Trust

Information Risk Security Policy

DOCUMENT INFORMATION	
CATEGORY:	Policy
THEME:	Information
DOCUMENT REFERENCE:	7.21
EXECUTIVE LEAD:	Director of Finance
APPROVAL DATE:	**28 April 2016**
APPROVAL BODY:	**Quality Committee**
BOARD RATIFICATION DATE:	**11 May 2016**
FINAL REVIEW DATE:	**31 May 2019**

This information will be completed by the Trust Secretary

Contents

Glossary

SIRO	Senior Information Risk Owner ISM	Information Security Manager
IAO	Information Asset Owner	
IAA	Information Asset Administrator	
IGM	Information Governance Manager	
ISM	Information Security Manager	
IAAF	Information Asset Audit Form (*Appendix A)*	

1. Policy Statement

Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the Trust continuously manages information risk. This policy recognises that the aim of information risk management is not to eliminate risk, but rather to provide the structural means to identify prioritise and manage the risks involved in all Trust activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived from using information appropriately.

Information risk management is an essential element of broader information governance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions.

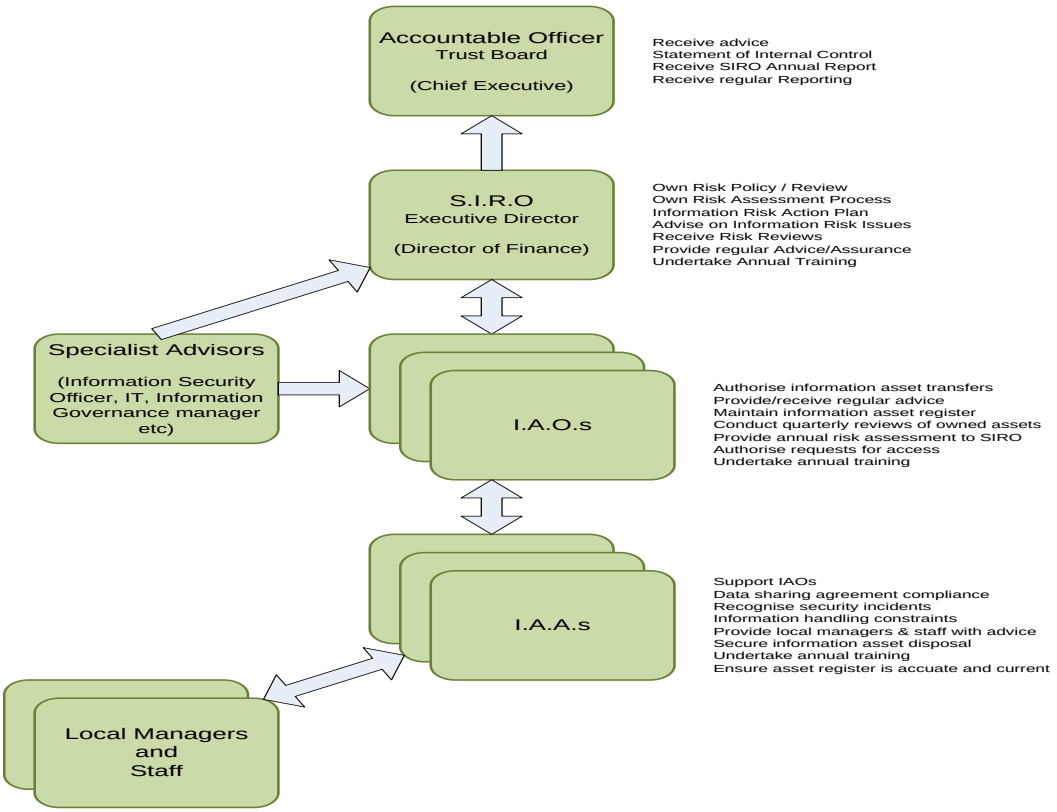
It should be noted that this policy complements and does not supersede the Trusts Risk Management Policy and Strategy documents.

2. Scope

This policy applies to all areas of the Trust and all individuals employed by the Trust, including contractors, voluntary workers, students, locum and agency staff.

When an Information Asset is identified an Information Asset Audit Forms (IAAF) will be completed *(see Appendix A)* containing a standard Trust Risk Assessment. This will be reviewed and, where necessary, updated annually. If any risks are escalated to a "high" rating; they should be reported and entered on the Trusts Risk Register. Risk Assessments should be completed in line with the Trusts Risk Management Policy and reviewed at regular intervals.

3. Duties



3.1 Chief Executive

The Chief Executive as the Accountable Officer for the Trust has overall accountability and responsibility for IG in the Trust and is required to provide assurance through the Statement of Internal Control that all risks to the Trust, including those relating to information, are effectively managed and mitigated. Details of Serious Untoward Incidents involving data loss or confidentiality breach must also be reported in the annual report.

3.2 Senior Information Risk Officer

The Director of Finance is responsible to the Chief Executive for IG and is the designated Senior Information Risk Owner (SIRO), who takes ownership of the Trust's Information Risk Policy, acts as advocate for information risk on the Board and provides written advice to the Accountable Officer on the content of the Statement of Internal Control in regard to information risk.

3.3 Caldicott Guardian

The Caldicott Guardian is the "conscience" of the organisation, providing a focal point for patient confidentiality and information sharing issues, and advising on the options for lawful and ethical processing of information as required. The Caldicott Guardian and SIRO are both concerned with ensuring NHS data is protected and is not stored, accessed or used inappropriately. The SIRO and any organisational IAOs work closely with the Caldicott Guardian and consult him/her where appropriate when conducting information risk reviews for assets which comprise or contain patient information.

3.4 Information Security Manager

The Information Security Manager (ISM) will be responsible to the SIRO and IAOs for the identification, delivery and management of an information risk management programme to address and manage risks to the Trusts Information Assets.

3.5 Information Asset Owners

Appropriate staff will be designated Information Asset Owners (IAOs) with responsibility for the completion and maintenance of the Trust's Information Asset Register; for providing assurance to the SIRO that information risks within their respective directorate have been identified and recorded, and that controls are in place to mitigate those risks. The Information Asset Audit Form (see Appendix A) will be completed/reviewed on an annual basis, for each asset, and forwarded to the ISM each year. This information will be collated to provide evidence for the IG Toolkit.

3.6 Information Asset Administrators

IAOs can appoint Information Asset Administrators (IAAs) to support them in the delivery of their information risk management responsibilities for the Directorate. IAAs ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.

3.7 Information Governance Manager

The IGM is responsible for managing the information Governance agenda across the Trust. This will include monitoring compliance with those requirements around Information Risk Management within the IG Toolkit and ensuring these standards are met.

3.8 All Staff

Everyone has a role in the effective management of information risk. All staff will actively participate in identifying potential information risks in their area and contribute to the implementation of appropriate treatment actions. All CHT employees and anyone else

working for CHT (e.g. agency staff, honorary contracts, management consultants etc.) who uses and has access to Trust information must understand their personal responsibilities for information governance and comply with the law. All staff must comply with Trust policies, protocols, procedures and guidance and attend relevant education and training events.

4. Framework

4.1 Policy objectives

The Information Risk Policy has been created to:

- Protect the Trust, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant;
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes; Encourage pro-active rather than re-active risk management;
- Provide assistance to and improve the quality of decision making throughout the Trust;
- Meet legal or statutory requirements; and
- Assist in safeguarding the Trust's information assets.

4.2 Information Security

The aim of Information Security is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Trust.

North Staffordshire Combined Healthcare is committed to achieving the following Information Security and IG objectives:

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training
- The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instance of actual or potential breaches of information confidentiality and security.

4.3 Information Assets

The guidance contained within this policy and its related materials applies to NHS information assets of all types. These information assets may consist of:

- Digital or hard copy patient health records (including those concerning all specialties and GP medical records);
- Digital or hard copy administrative information (including, for example, personnel, estates, corporate planning, supplies ordering, financial and accounting records);
- Digital or printed X-rays, photographs, slides and imaging reports, outputs and images;
- Digital media (including, for example, data tapes, CD-ROMs, DVDs, USB disc drives, removable memory sticks, mobile phones and other internal and external media compatible with NHS information systems);
- Computerised records, including those that are processed in networked, mobile or standalone systems;
- Email, text and other message types.

4.4 Training

The Connecting For Health - IG Training Tool is an online training tool focused on all aspects of learning about Information Governance (IG). The aim of the tool is to develop and improve staff knowledge and skills in the IG work area.

The Trust's Information Risk Management programme will require the SIRO, IAO and IAA to complete the following online modules. Non-compliance will be escalated to line managers if modules are not completed within a reasonable timeframe.

The ISM will monitor and maintain a training matrix of the required modules per person as shown in the example below:

Key
Red - Nationally Mandated
Orange - Locally Mandated

	Caldicott Guardian	Senior Information Risk Officer	Information Security Manager	Information Asset Owner	Information Asset Administrator
Patient Confidentiality				per asset	per asset
The Caldicott Guardian in the NHS and Social Care					
NHS Info Risk Mgt: Intro				per asset	per asset
NHS Info Risk Mgt: Foundation				per asset	per asset
NHS Info Risk Mgt for SIROs and IAOs				per asset	per asset
Secure Transfers of Personal Data				per asset	per asset
Info Security Mgt				per asset	per asset
Business Continuity Mgt				per asset	per asset
Records Mgt and the NHS Code of Practice				per asset	per asset

4.5 Key definitions are:

- **Risk**
  The chance of something happening which will have an impact upon objectives. It is measured in terms of *consequence* and *likelihood*.
- **Consequence**
  The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain.
- **Likelihood**
  A qualitative description or synonym for probability or frequency.
- **Risk Assessment**
  The overall process of risk analysis and risk evaluation.
- **Risk Management**
  The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
- **Risk Treatment**
  Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:
    - Avoid the risk
    - Reduce the likelihood of occurrence
    - Reduce the consequences of occurrence
    - Transfer the risk
    - Retain/accept the risk

- **Risk Management Process**

  The systematic application of management policies, procedures and practices to the task of establishing the context, identifying, and analysing, evaluating, treating, monitoring and communicating risk.

5. Implementation and Monitoring

The Information Risk Management process will be reviewed annually against the NHS Connecting for Health IG Toolkit to identify key areas for continuous improvement. Specific elements relating to this policy are:

8-300	The information governance agenda is supported by adequate information security skills, knowledge and experience which meets the organisation's needs.
8-301	A formal information security risk assessment and management programme for key information assets has been documented, implemented and reviewed.
8-302	There are documented information security incident/event reporting and management procedures that are accessible to all staff.
8-308	All transfers of hardcopy and digital person identifiable and sensitive information have been identified, mapped and risk assessed, and technical and organisational measures adequately secure these transfers.
8-323	All information assets that hold or are personal data are protected by appropriate organisational and technical measures.

The IG Toolkit contains guidance on expected standards and key performance indicators, which together will be used to monitor the effectiveness of this policy and the Information Risk Management programme. Reports will be generated to monitor the training within the IG Toolkit.

6. Associated Policy and Procedural Documentation

6.1 Related policies/guidelines – Local

This document should be read in addition to the following policies found on the Trust Intranet website (SID)

Risk Management Policy
Risk Management Strategy
Information Security & Data Protection Policy
Mobile Information Handling Policy
Safe Haven Policy
Incident Reporting Policy
IT Asset Management Policy
Data Quality Policy
Information Governance Assurance Framework
Transport Documentation Procedure (red, yellow and green bags)

6.2 Related policies/guidelines – National

Department of Health Information Security Management NHS Code of Practice – April 2007

NHS Information Risk Management Digital Information Policy – January 2009

Data Protection Act 1988

7. Incident Reporting

The reporting of Serious Incidents (including Cyber Incidents) relating to potential or actual breaches of confidentiality involving person identifiable data, including data loss, will be in line with the Trusts overall incident reporting processes, following the procedure outlined in the Trusts Incident Reporting Policy, and via the IG Toolkit for any incidents hitting Level 2 or above.

Appendix A

INFORMATION ASSET AUDIT FORM - to be completed by the Information Asset Owner (IAO)				
Directorate:			Location:	
Department/Service:				
Information Asset Owner:			Tel No:	

1	Name of the Information Asset			
2	Description of the Information Asset			
3	Who is the supplier, and if external is there a maintenance agreement?	In house ☐ External supplier ☐ Please supply details		
4	Is there a Business Continuity Plan	Yes ☐ No ☐	Where is it stored?	
5	Do you feel that a Risk Assessment is necessary for this information asset?	Yes ☐ No ☐	Please complete Risk Assessment over page Please state reason	
6	Is access to the information asset shared within the Trust?	No ☐ Yes ☐	If 'Yes', with whom is it shared? Does it include access to personal data? Yes ☐ No ☐ Why is it shared? Do you follow the Trust's Incident Reporting Guidelines should an incident occur? Yes ☐ No ☐	
7	Is access to the information asset shared with an external organisation outside of the Trust?	No ☐ Yes ☐	If 'Yes', with whom is it shared? Does it include access to personal data? Yes ☐ No ☐ Why is it shared? Is there a Sharing Agreement in place? Yes ☐ No ☐ Do you have confirmation from the receiving organisation that they are IG compliant? Yes ☐ No ☐ Do you follow the Trust's Incident Reporting Guidelines should an incident occur? Yes ☐ No ☐	
8	Who is the responsible Information Asset Administrator (IAA)	Name: Job Title: Tel No:		

Information Asset Owner Signature..... Date.....

Please note: If you are registered as a 'Sole Owner' i.e. IAO *and* IAA, for an information asset, please complete both forms and add a statement in section 13 regarding responsibility in the event of your absence.

Comments
If you have any further comments to the questions above please note in this section:

Information Asset Risk Assesment

Guidance:

- *Determine the Likelihood of risk from the matrix and enter the corresponding figure into the lilac cell at the bottom of the table*
- *Determine the Impact or Consequence of the risk from the chart and enter the corresponding figure into the lilac cell at the bottom of the table*
- *The risk calculator will calculate the risk score and return the appropriate RAG rating for the score*
- *Confirm the correct calculation for final risk score (e.g 3x2=6 = Green) on Risk Calculator*

Please Note that risks of AMBER or RED will need a full Risk Assessment to be completed and entered separately onto the Operational Risk Register (see Risk Management Policy on SID for guidance and risk assessment form)

Likelihood

Rare = 1	Unlikely = 2	Possible = 3	Likely = 4	Almost Certain = 5
This will probably never happen/recur	Do not expect it to happen/recur but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur but it is not a persisting issue	Will undoubtedly happen/recur, possibly frequently
1				

Impact or Consequence

Descriptor	Insignificant = 1	Minor = 2	Moderate = 3	Major = 4	Catastrophic = 5
Information Security - Breach of Confidentiality	Potentially serious breach. Less than 5 people affected or risk assessed as low, e.g. files were encrypted	Serious potential breach and risk assessed high e.g. unencrypted clinical records lost. Up to 20 people affected	Serious breach of confidentiality e.g. up to 100 people affected	Serious breach with either particular sensitivity e.g. sexual health e.g. sexual health details, or up to 1000 people affected	Serious Breach with potential for ID theft or over 1000 people affected.
Score			3		

Risk Matrix

	Likelihood				
Consequences	Rare	Unlikely	Possible	Likely	Almost Certain
Catastrophic = 5	5	10	15	20	25
Major = 4	4	8	12	16	20
Moderate = 3	3	6	9	12	15
Minor = 2	2	4	6	8	10
Insignificant = 1	1	2	3	4	5

Risk Calculator (Do not enter data into these boxes)

Likelihood	1
Consequence	3
Risk Score	3

INFORMATION ASSET AUDIT FORM - to be completed by Information Asset Administrator - (IAA)

Directorate: | **Location:**

Department/Service:

Information Asset Administrator: | **Tel No:**

1	**Name of the Information Asset**		
2	**Are duplicates of the information asset held?**	Yes ☐ No ☐	**If 'Yes', where?**
3	**Why do you create/collect this information?** Please tick all that apply	Patient care /admin ☐ Clinical audit ☐ Central returns ☐ Business/Corporate ☐ Statutory Requirement	Research ☐ Other ☐ Please specify:
4	**Where does the information come from?**	Generated within the dept. (e.g. from patients, staff etc.) ☐ Transferred from **within** the Trust ☐ Transferred from **outside** the Trust ☐	
5	**How many records are held? (Estimate)**		
6	**Is the information asset in a 'Safe Haven'**	Yes ☐ No ☐	
7	**Is the data password protected?**	Yes ☐ No ☐	**If 'Yes', is it further restricted by job title etc.? (please specify)**
8	**Where is the data held?**	**Local Hard Drive** ☐	Why? Is there a Business Continuity Plan? Yes ☐ No ☐
		NHS CHC Network X Drive ☐	
		DVD CD ROM USB Memory Stick or External Hard Drive ☐	Why? Is there a Business Continuity Plan? Yes ☐ No ☐
		Other ☐	(Please specify)
9	**Is there a back up system?**	Yes ☐ No ☐ Don't know ☐	**If 'Yes', specify** Note: NHS CHC Network X Drive is backed up daily
10	**Do you have a record tracking system should records leave the department?**	Yes ☐ No ☐	If 'Yes', is it: Paper based ☐ Electronic ☐
11	**Have you identified how long the records are retained?**	Yes ☐ No ☐	
12	**What action is taken when the retention period is exceeded?**	Deleted ☐	**How?**
		No action taken ☐	**Why?**
		Archived elsewhere ☐	**Where?**
		Other ☐	**Specify**

13

If you have any further comments or questions regarding the Information you hold (e.g. Creation, maintenance, storage, retention, disposal etc.) please specify below:

Sole Owners' i.e. IOA *and* IAA - please add a statement below regarding responsibility in the event of your absence

Information Asset Owner Signature..... Date.....

Information Asset Administrator Signature..... Date.....

Please return your form to your IAO for signature

INFORMATION ASSET AUDIT FORM

Completion Guidance for Information Asset Owners (IAO)

Information Asset Owners are directly accountable to the Senior Information Risk Owner and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. Information Asset Owners may be assigned ownership of several assets of their organisation.

Please note that text boxes have limited input - please add extra information to the comments box at the end of the questionairre

1	**Name of the Information Asset**	Title by which the information asset is commonly known, e.g.: Trust Case notes, X-Ray images etc.
2	**Description of the record**	Brief description of the information showing the role and purpose and any other important intellectual or physical characteristics. This field may include background and uses of the information. Ideally this should be two or three sentences in length, but accuracy is more important than length.
3	**Who is the supplier, and if external is there a maintenance agreement**	For any systems that are not 'in house' , i.e. CHC systems, state the name of the company. (E.g. OIT UK) with contact details, telephone number etc. The maintenance agreement should contain details such as call out procedures, timeframes, response times, frequency of renewal etc. You may be asked to upload a copy of this document as evidence for the IG Toolkit submission.
4	**Is there a Business Continuity Plan**	This would be a set of documents, instructions, and procedures which enable the Trust (your department) to respond to accidents, disasters, emergencies, and/or threats without any stoppage or hindrance in its key operations. Business Continuity Plans, including contingency and recovery plans,(disaster recovery plans) help NHS organisations to reduce the effects of disruption upon services, systems and business processes caused by service interruptions and failures. Does your department have a process to manually collect the required information should the electronic system fail, and if so, are you aware where this is this documented and what is the process to be followed?The Plan should be reviewed annually.
5	**Is there a Risk Assessment**	It is for you to decide if this information asset warrants a risk assesment based on the size, content, access and use of the information. If so then please complete the Information Asset Risk Assessment form on the second page of the form. If you feel the asset does not need a risk assessment please state why e.g. 'small department staff database'. For more information see the Trust's Risk Management Policy No. 4.18 on SID. If you have any queries about the process please contact your divisional Risk Lead who can assist you with completion. Risk Leads are: Joanne Orlando - Adult Mental Health, Lisa Wilkinson - LD and NOAP, Nicola Butcher - CAMHS.
6	**Is access to the information asset shared within the Trust**	Which members of the organisations staff can read the information within the record? Can they access confidential personal information? Is there a 'need to know' this data?
7	**Is access to the information asset shared with an external organisation outside of the Trust?**	Which members of staff from other organisations can read the information within the record? Can they access confidential personal information? Is there a 'need to know' this data? You may be asked to upload a copy of the Sharing Agreement and/or Compliance Statement as evidence for the IG Toolkit submission.
8	**Who is the responsible Information Asset Owner (IAA)**	You now need to nominate an Information Asset Administrator (IAA) from your Department. The IAA is usually an operational member of staff who understands and is familiar with information risks in their area or department, e.g. Security Managers, Records Managers, Data Protection Officers, Internal Audit. An appropriate operational role may include Office or Departmental Managers, Shift Supervisors and senior administrative staff. The IAA will implement the organisations Information Risk Policy and risk assessment process for those information assets they support and will provide assurance reports to the relevant Information Asset Owner as necessary.

Please note: If you are registered as the 'Sole Owner' i.e. IAO *and* IAA, for an informaiton asset, please complete both forms and add a statement in section 13 regarding responsibility in the event of your absence

INFORMATION ASSET AUDIT FORM

Completion Guidance for Information Asset Administrators (IAA)

Information Asset Administrators are usually operational members of staff who understand and are familiar with information risks in their area or department, e.g. Security Managers, Records Managers, Data Protection Officers, Internal Audit. For smaller organisations, an appropriate operational role may include Office or Departmental Managers, Shift Supervisors and senior administrative staff. Information Asset Administrators will implement the organisation's information risk policy and risk assessment process for those information assets they support and will provide assurance reports to the relevant Information Asset Owner as necessary.

1	**Name of the Information Asset**	Title by which the information asset is commonly known, e.g.: Trust Case notes, X-Ray images etc.
2	**Are duplicates of the information held**	Are the same records kept in, for example, another department or a different format e.g. paper documents etc.?
3	**Why do you create/collect this information**	All information collected by a Trust must be for a purpose, particularly confidential data. Use the 6 broad categories (more than 1 category can be selected) and the 'Other' box for more specific uses of information.
4	**Where does the information come from**	Is the information collected within the department or transferred from within or from outside the organisation?
5	**How many records are held? (Estimate)**	How many records are contained within the collection?
6	**Is the information asset in a 'safe haven'**	A 'safe haven' is a term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the Trust to ensure confidential patient or staff information is communicated safely and securely. It is a safeguard for confidential information, which enters or leaves the Trust, whether this is by facsimile (fax), post, email or any other means. Any members of staff handling confidential information, whether paper based or electronic, must adhere to the Safe Haven principles. See CHC Safe Haven Policy 7.14 for more detailed definition.
7	**Is the data password protected?**	Passwords are the keys that open electronic doors and they are the main protection against unauthorised access to data and information held on computers. To access the records, is a password required?
8	**Where is the data held?**	This question is to identify location of records/information (e.g. a Trust computer network, standalone computer or on CD/DVD/Memory Stick). If information is stored on a Local Hard Drive (e.g. your own user drive on your work computer rather than the network X Drive) or any external equipment, such as a USB memory stick, you need to state the reason why this is.
9	**Is there a back up system?**	A back up system allows data essential to the business of the organisation to be restored or recovered as quickly as possible in the event of data loss or corruption on one or more of its computer systems. In order to achieve this, data is copied to a medium that can then be safely stored in a secure place on a frequent and regular cycle. **Note: If Data is stored on CHC X Drive this is automatically backed up on a regular basis**
10	**Do you have a record tracking system should records leave the department?**	The ability to track/trace electronic records once they leave storage is essential. Tracking systems can be either paper-based or electronic.
11	**Have you identified how long the records are retained?**	Annexes D1 (Health Records) and D2 (Business & Corporate Records) of the NHS Code of Practice for Records Management set out minimum retention periods for all types and categories of NHS records. Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time.
12	**What action is taken when the retention period is exceeded?**	Annex D of the NHS Code of Practice for Records Management (Section 3) sets out the final action that apply at the end of the relevant minimum retention periods and also provides guidance, in Section 5, on who should make decisions regarding the disposal and destruction of records.
13	**Further Comments**	Please document and concerns, suggestions etc. regarding the management or security of records.